Change Auditor Threat Detection

Proaktive Erkennung von Bedrohungen durch Benutzer für Microsoft-Umgebungen

Die große Mehrheit der Unternehmen verlässt sich auf Active Directory (AD) als primäre Quelle für Authentifizierung und Autorisierung, wodurch es zum Hauptziel von Hackern, Cyberterroristen und verärgerten Ex-Mitarbeitern wird. Doch Unternehmen erkennen möglicherweise nicht, das eine viel unmittelbarere Bedrohung für ihre AD-Sicherheit tatsächlich – sowohl bewusst als auch unbewusst – aus den eigenen Reihen kommt. Noch schlimmer ist, dass es aufgrund der Komplexität von AD extrem schwierig ist, Bedrohungen zu erkennen, wenn sie auftreten. Und herkömmliche regelbasierte Ansätze zur Erkennung von Bedrohungen durch Benutzer generieren so viele Warnungen, dass man unmöglich allen nachgehen kann. Sie riskieren, echte Bedrohungen komplett zu verpassen, und setzen Ihr Unternehmen so der Gefahr von Datensicherheitsverstößen aus. Aber wie können Sie alle Benutzeraktivitäten in Ihrer Umgebung in Echtzeit analysieren, um Ihr Unternehmen vor Unterbrechungen und Ausfällen zu schützen?

Change Auditor Threat Detection bietet einen einzigartigen Ansatz zur Erkennung von Bedrohungen durch Benutzer, indem Verhaltensmuster einzelner Benutzer in Modellen dargestellt werden, um außergewöhnliche Aktivitäten zu erkennen, die auf verdächtige Benutzer oder kompromittierte Konten hinweisen könnten. Durch Analyse der Benutzeraktivitäten mit eigener fortschrittlicher Lerntechnologie, Verhaltensanalysen einzelner Benutzer und Gruppen sowie aufwändige Bewertungsalgorithmen, stuft Change Auditor Threat Detection die Benutzer in Ihrem Unternehmen ein, von denen die größte Gefahr ausgeht, erkennt mögliche Bedrohungen durch Benutzer und verringert überflüssige Warnungen. Schließlich werden Sie in der Lage sein, die Lücke zu schließen, die native Prüftools hinterlassen haben, und so Ihre Umgebung sicher zu halten.

FUNKTIONEN

Echtzeit-Analyse von Prüfprotokollen

Analysieren Sie effizient große Mengen von Prüfdaten wie Veränderungen,

Change Auditor Threat Detection hilft Ihnen, verdächtige Benutzeraktivitäten schnell und einfach zu erkennen, damit Ihre Umgebung und Benutzer geschützt sind.

VORTEILE:

- Proaktive Erkennung von Bedrohungen auf Grundlage von Benutzerverhaltensmustern
- Verringerung der Anzahl von Warnungen in Verbindung mit regelbasierter Bedrohungserkennung
- Anzeige von Sicherheitswarnungen im Kontext zur schnellen und einfachen Bestimmung ihrer Schwere
- Einfache Erkennung außergewöhnlichen Benutzerverhaltens mit Benutzerverhaltensgrundlagen
- Bedrohungserkennung auf Grundlage Ihrer bestehenden Prüfdaten zur Minimierung der Auswirkungen auf Ihre Infrastruktur

ANWENDUNGSBEISPIELE:

Change Auditor Threat Detection ermöglicht es Ihnen, schnell und einfach solche Bedrohungen zu erkennen wie:

- Ungewöhnliche AD Aktivitäten
- Missbrauch privilegierter Konten
- Brute-Force-Angriffe
- Datenfilterung
- Unangemessener Zugriff auf System oder Ressourcen
- Malware
- Rechteerweiterung
- Lateral Movement

SYSTEMANFORDERUNGEN

CHANGE AUDITOR KOORDINATOR

(Serverseitige Komponente)

Prozessor: Quad-Core Intel Core i7 entsprechend oder höher

Arbeitsspeicher: Minimum: 8 GB RAM oder höher; empfohlen: 32 GB RAM oder höher

CHANGE AUDITOR CLIENT

(Clientseitige Komponente)

Prozessor: Dual-Core Intel Core i5 entsprechend oder höher

Arbeitsspeicher: Minimum: 4 GB RAM oder höher; empfohlen: 8 GB RAM oder höher

CHANGE AUDITOR AGENT

(Serverseitige Komponente)

Prozessor: Dual-Core Intel Core i5 entsprechend oder höher

Arbeitsspeicher: Minimum: 4 GB RAM oder höher; empfohlen: 8 GB RAM oder höher

Eine detaillierte und aktuelle Liste der Systemanforderungen finden Sie auf support.quest.com/change-auditor

Authentifizierungen und Dateiaktivitäten bei AD. Entwickeln Sie aus diesen Aktivitätsvorkommen Benutzergrundlagen und erkennen Sie proaktiv, wenn außergewöhnliches Benutzerverhalten auftritt, damit Ihnen mögliches verdächtiges Verhalten umgehend bekannt wird.

Automatische Benutzerverhaltensanalysen

Modellieren Sie Benutzerverhaltensmuster, die kein Zutun vom Administrator und keine Konfiguration erfordern. Benutzerverhaltensgrundlagen werden mittels nicht überwachter fortschrittlicher Lerntechnologe automatisch erstellt, indem jeder Aspekt der Aktivitäten eines Benutzers modelliert wird. Dazu gehören dessen Anmeldemuster, Verwaltungsaktivitäten sowie Zugriff auf Dateien und Ordner.

Fortschrittliche Erkennung außergewöhnlichen Verhaltens

Erkennen Sie außergewöhnliche Benutzeraktivitäten durch einen automatischen Vergleich sämtlicher Benutzeraktivitäten mit der Verhaltensgrundlage des betreffenden Benutzers. Eine fortschrittliche Erkennung von Bedrohungsanzeichen sowie eine Risikobewertung auf verschiedenen Ebenen stellen sicher, dass nur auf die außerordentlichsten Anomalien hingewiesen wird, wodurch das gefährlichste Benutzerverhalten widergespiegelt wird.

Musterbasierte Erkennung von Bedrohungen durch Benutzer

SMART-Warnungen vor Bedrohungen durch Benutzer werden nur ausgegeben, wenn ein korreliertes Muster außergewöhnlichen Benutzerverhaltens festgestellt wird. Anstatt sich darauf zu verlassen, dass anhand von Regeln bestimmte Aktivitäten erkannt werden, werden automatisch sämtliche Benutzeraktivitäten in Echtzeit analysiert und die verdächtigsten Benutzer in der Umgebung durch fortschrittliche Erkennung von Verhaltensmustern ermittelt. Eine fortschrittliche ganzheitliche Modellierung sorgt dafür, dass nur die kritischsten und besorgniserregendsten Benutzerverhaltensmuster aufgezeigt werden, wodurch das Aufsehen wegen isolierter Aktivitäten und falscher Treffer erheblich verringert wird.

Getreue Benutzeranalysen

Change Auditor erstellt die Prüfprotokolle, anhand derer die Analysen durchgeführt werden. Daher enthalten alle unverarbeiteten Ereignisdaten zur proaktiven Erkennung von Bedrohungen in Ihrer Umgebung grundsätzlich wertvolle so Informationen wie:

- Wer die Änderung vorgenommen hat
- Was geändert wurde
- Wann es geändert wurde
- Wo es geändert wurde
- Und die IP-Adresse oder Workstation, von wo die Änderung stammt

Im Gegensatz zu nativen Windows-Ereignisprotokollen stellt Change Auditor sicher, dass keine wichtigen Benutzeraktivitäten verpasst werden, was andernfalls kritische Lücken bei den Benutzerverhaltensanalysen zur Folge hätte.

Sicherheitswarnungen im Kontext

Zeigen Sie alle verdächtigen Benutzeraktivitäten im Kontext der Bedrohungsanzeichen an, die in der Warnung enthalten waren. Jedes außergewöhnliche Verhalten wird im Kontext der Grundaktivitäten des betreffenden Benutzers und mit allen unverarbeiteten Ereignissen dargestellt, die die Warnung ausgelöst haben. So wird deutlich, warum die Warnung ausgegeben wurde. Zudem werden die Untersuchung und Nachbereitung vereinfacht.

Leichte Erkennung von Bedrohungen durch Benutzer

Nutzen Sie Ihre bestehende Change Auditor-Infrastruktur und Prüfdaten, um Benutzerverhalten zu modellieren, damit keine unnötig schwerfälligen zusätzlichen Agenten und Server bereitgestellt zu werden brauchen. Eine einzelne virtuelle Appliance ist die einzige erforderliche zusätzliche Infrastruktur, um fortschrittliche Analysen von Bedrohungen durch Benutzer durchführen zu können.

ÜBER QUEST

Bei Quest versuchen wir, komplexe Herausforderungen mit einfachen Lösungen zu bewältigen. Dies gelingt uns dank unserer speziellen Unternehmensphilosophie, bei der hervorragender Service und unser allgemeines Ziel – ein unkomplizierter Geschäftspartner zu sein – im Vordergrund stehen. Unsere Vision besteht darin, Technologien bereitzustellen, bei denen Sie sich nicht zwischen Effizienz und Effektivität entscheiden müssen. Dadurch müssen Sie und Ihre Organisation sich weniger um die IT-Verwaltung kümmern und haben mehr Zeit für Unternehmensinnovation.

Quest
www.quest.com/de
Kunden außerhalb Nordamerikas finden Informationen zu lokalen Niederlassungen auf unserer Website.

DataSheet-ChangeAuditorThreatDetection-US-KS-DE-WL-32855